AD/A-005 691

ON A COVERING PROBLEM FOR PARTIALLY SPECIFIED SWITCHING FUNCTIONS

M. Schkolnick

Carnegie-Mellon University

Prepared for:

Air Force Office of Scientific Research
Defense Advanced Research Projects Agency

December 1974

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFOSR - TR - 75 - 0195	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER AD/A005 691
4. TITLE (and Subtitle) ON A COVERING PROBLEM FOR PARTIALLY SPECIFIED SWITCHING FUNCTIONS		5. TYPE OF REPORT & PERIOD COVERED Interim
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) M. Schkolnick		8. CONTRACT OR GRANT NUMBER(s) F44620-73-C-0074
9. PERFORMING ORGANIZATION NAME AND ADDRESS Carnegie-Mellon University Computer Science Dept. Pittsburgh, PA 15213		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 61101D AO-2466
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Advanced Research Projects Agency 1400 Wilson Blvd. Arlington, VA 22209		12. REPORT DATE December 1974
		13. NUMBER OF PAGES ~~8~~ 10
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Air Force Office of Scientific Research (NM) 1400 Wilson Blvd. Arlington, VA 22209		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

We consider the problem of finding the minimum number K(n,c) of total switching functions of n variables necessary to cover the set of all switching functions which are specified in at most c positions. We find an exact solution of K(n,2) and an upper bound for K(n,c) which is better than a previously known upper bound by an exponential factor.

(10)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ON A COVERING PROBLEM
FOR PARTIALLY SPECIFIED SWITCHING FUNCTIONS

M. Schkolnick
Carnegie-Mellon University
Pittsburgh, Pa. 15213

December 1974.

Abstract

We consider the problem of finding the minimum number $K(n,c)$ of total switching functions of n variables necessary to cover the set of all switching functions which are specified in at most c positions. We find an exact solution for $K(n,2)$ and an upper bound for $K(n,c)$ which is better than a previously known upper bound by an exponential factor.

This work was supported by the Defense Advanced Research Projects Agency
under Contract F44620-73-C-0074.

10

1. Introduction

The problem considered here can be stated as follows:

P1: Given the set F of all c-specified boolean functions of n variables, i.e., all functions which are specified in at most c positions, to find the cardinality $K(n,c)$ of a set G of total functions such that

P1-1: For all f in F, there is a g in G such that g covers f, i.e., if $f(x)$ is specified then $g(x) = f(x)$.

P1-2: $K(n,c) = |G|$, is minimal.

This problem relates the number of additional exterior connections (besides input and output) that are required in a circuit which is to be c-universal. (A circuit is c-universal if it is capable of simulating the behavior of any partial function which is specified in c or less points of its domain.)

This problem was studied in [1] in connection with adaptive networks, where an upper bound for $K(n,c)$ was shown to be

$$K(n,c) \leq \sum_k \binom{m}{p+k\delta}$$

where $m = 2^n$, $p = \lfloor c/2 \rfloor \bmod \delta$, $\delta = m+1-c$

This upper bound agrees with the exact solutions for $c=1$ (i.e., $K(n,1)=2$) and $c=2^n-1$ (i.e., $K(n,2^n-1)=2^{2^n-1}$). For $c=2$ we have $\delta=2^n-1$ and, for any $n > 1$, $p=1$ so

$$K(n,2) \leq \sum \binom{2^n}{1+k(2^n-1)} = \binom{2^n}{1} + \binom{2^n}{2^n} = 2^n + 1$$

and in general, for small c, this bound is of the order of $2^{nc/2}$.

In this note we show that for $c=2$, $K(n,2) = O(n)$ and present an upper bound which, for fixed c is a power of n.

2. An Exact Solution for $K(n,2)$

Consider the following problem:

P2: Given n and c, find the dimension $s(n,c)$ of a vector space over GF(2) such that there is a set P of at least 2^n vectors in it satisfying:

P2-1: $(\forall p_1,p_2,...,p_c) \in P$, $(\forall b_1,b_2,...,b_c) \in \{0,1\}$, $p_1^{b_1} p_2^{b_2} \dots p_c^{b_c} \neq \underline{0}$

P2-2: $s(n,c)$ is minimal

Notation: We will use the following convention

1) $(\forall a,b,...,z) \in M$ means for all elements $a,b,...,z$ in M.

2) p^b = if $b=1$ then p else $\sim p$

The first result we present shows that essentially, P1 and P2 are equivalent problems.

Lemma 1: For all $c > 1$, $K(n,c) = s(n,c)$.

Proof: We show that any solution to P1 satisfying P1-1 is a solution to P2 satisfying P2-1 and conversely. This implies that the minimality conditions are also satisfied.

Let $G = \{g_1,g_2,...,g_{K(n,c)}\}$ be a solution to P1 satisfying P1-1. Consider the set $P = \{p(x) = (g_1(x),g_2(x),...,g_{K(n,c)}(x)) | x \in \{0,1\}^n\}$. Let $x,y \in \{0,1\}^n$ with $x \neq y$. Then $p(x) = p(y) \Rightarrow (\forall g) \in G$, $g(x) = g(y)$. But since $c > 1$, this implies that there is a c-specified function f with $0 = f(x) \neq f(y) = 1$ which is not covered by any $g \in G$ which is a contradiction. Thus $p(x) \neq p(y)$, which shows that $|P| = 2^n$.

Assume now that there are c different elements $p_1,p_2,...,p_c$ in P such that, for some $b_1,b_2,...,b_c \in \{0,1\}$, $p_1^{b_1} p_2^{b_2} \dots p_c^{b_c} = \underline{0}$. Let $p_j = p(x_j) = (g_1(x_j),g_2(x_j),...,g_{K(n,c)}(x_j))$ for some n-tuple $x_j \in \{0,1\}^n$. Let f be a c-specified function such that $f(x_j) = b_j$ for $j = 1,2,...,c$. Since $p_1^{b_1} p_2^{b_2} \dots p_c^{b_c} = \underline{0}$, for each $k = 1,2,...,K(n,c)$, there is a j, $1 \leq j \leq c$ such that $g_k(x_j) = 1-b_j$. Thus, for this value of j we have $g_k(x_j) \neq f(x_j)$ so g_k does not cover f. Since this holds for all k, we have that G does not satisfy P1-1, a contradiction. Thus, P2-1 is satisfied.

Conversely, let P be a set of 2^n s-dimensional vectors $P = \{p_\emptyset, p_1, p_2, \dots, p_{2^n-1}\}$ satisfying P2-1. Consider the set $G = \{g_1, g_2, \dots, g_s\}$ of boolean functions of n variables defined as follows:

For each $1 \leq j \leq s$, $(\forall i) \in \{\emptyset, 1, \dots, 2^n-1\}$, $g_j((\underline{i}_2)_1, (\underline{i}_2)_2, \dots, (\underline{i}_2)_n) = (p_i)_j$ where $\underline{i}_2$ denotes the binary representation of i with n bits, $(\underline{i}_2)_r$ denotes the r-th bit and for an s-dimensional vector p, $(p)_r$ denotes the r-th component.

Let f be a c-specified function of n variables. Without loss of generality, assume that f is specified at $((\underline{i}_2)_1, (\underline{i}_2)_2, \dots, (\underline{i}_2)_n)$ for $i = \emptyset, 1, \dots, c-1$. We claim there is at least one g which covers f. Define, for $i = \emptyset, 1, \dots, c-1$, $b_i = f((\underline{i}_2)_1, (\underline{i}_2)_2, \dots, (\underline{i}_2)_n)$. Since P satisfies P2-1, $p_\emptyset^{b_\emptyset} p_1^{b_1} \dots p_{c-1}^{b_{c-1}} \neq \underline{\emptyset}$. Thus, there is a $j \in \{1, 2, \dots, s\}$ such that, for all $i \in \{\emptyset, 1, \dots, c-1\}$, $(p_i^{b_i})_j = 1$. (Note that $p_i^{b_i}$ is either p_i or its complement, and this means the j-th component of this vector is 1.) This means that $(p_i)_j = b_i$. By the definition of b_i and the definition of G we have

$$g_j((\underline{i}_2)_1, (\underline{i}_2)_2, \dots, (\underline{i}_2)_n) = f((\underline{i}_2)_1, (\underline{i}_2)_2, \dots, (\underline{i}_2)_n)$$

for all $i \in \{\emptyset, 1, \dots, c-1\}$. Thus, $g_j \in G$ covers f. This completes the proof of Lemma 1. ▮

Now we focus our attention to Problem 2. In what follows, we assume s is restricted to be even and we will show that K(n,2) can be determined exactly (to within 1). We first prove an auxilliary result. Since P2 can be interpreted as: Find the smallest s such that there are at least 2^n points in the s-cube satisfying P2-1, we will now show that the search for points in the s-cube satisfying P2-1 can be reduced to the set of all points in the middle plane (i.e., having weight s/2).

Lemma 2: Let $c = 2$, s be an even positive number, and P be a set of s-dimensional vectors satisfying P2-1. Then, there is a set Q of s-dimensional vectors, each of which has weight $s/2$ and such that $|Q| = |P|$, satisfying P2-1.

Proof: We can assume, without loss of generality, that all vectors in P have weight $\geq s/2$. (It is clear that changing a vector by its complement in any set satisfying P2-1 also produces a set satisfying P2-1.) If all vectors have weight $s/2$ we have proved the lemma. Assume then that P contains t vectors $p_1, p_2, \ldots, p_t$ with maximal weight $u > s/2$. We will construct a set P' such that all vectors in it will have weights w such that $s/2 \leq w < u$. Since $u - s/2$ is finite this will prove the lemma.

Choose any set of t vectors $q_1, q_2, \ldots, q_t$ with the property that $q_i < p_i$ for $i = 1, 2, \ldots, t$ and such that the weight of each q_i is $u-1$.

Claim The set $P' = P \cup \{q_1, q_2, \ldots, q_t\} - \{p_1, p_2, \ldots, p_t\}$ is the required set.

To show the claim, we first note that there are always t vectors q_i as above. This follows directly from the relationship which exists between points in the s-cube.

Next we show that for any p_j, $j = 1, 2, \ldots, t$ and for any p^b, $p \in P - \{p_1, p_2, \ldots, p_t\}$, $w(p_j p^b) \geq 2$, where $w(p)$ denotes the weight of a boolean vector p. This follows because $w(p_j p^b) = w(p_j) + w(p^b) - w(p_j + p^b) \geq u + (s-u+1) - (s-1) = 2$. We then have that $w(g_j p^b) = w(p_j(\sim a_j)p^b) = w(p_j p^b) + w(\sim a_j) - w(p_j p^b + \sim a_j) \geq 2 + (s-1) - s = 1$ and so $g_j p^b \neq \emptyset$. (Here a_j is an atom such that $a_j < p_j$ and $q_j = p_j(\sim a_j)$.) Similarly, $w(\sim q_j p^b) = w((\sim p_j + a_j)p^b) = w(\sim p_j p^b + a_j p^b) \geq w(\sim p_j p^b) \geq 1$.

This means that any vector q and any vector in $P - \{p_1, \ldots, p_t\}$ satisfies P2-1. Clearly, any two vectors in $P - \{p_1, \ldots, p_t\}$ satisfy P2-1, so it remains to be shown that any two vectors in $\{q_1, q_2, \ldots, q_t\}$ satisfy P2-1.

We have $w(\sim q_i \sim q_j) = w((\sim p_i + a_i)(\sim p_j + a_j)) \geq w(\sim p_i \sim p_j) \geq 1$.

Also $w(\sim q_i q_j) \geq 1$ since $q_i \neq q_j$ and $w(q_i) = w(q_j) > s/2$. Finally, $w(q_i q_j) = w(p_i(\sim a_i)\ p_j(\sim a_j)) = w(p_i p_j) + w(\sim a_i \sim a_j) - w(p_i p_j + \sim a_i \sim a_j)$.

Since $w(p_i) = w(p_j) = u > s/2$,

$w(p_i p_j) = w(p_i) + w(p_j) - w(p_i + p_j) \geq (s/2+1) + (s/2+1) - (s-1) = 3$

So $w(q_i q_j) \geq 3 + (s-2) - s = 1$. This completes the proof of the lemma. ∎

Lemma 2 makes the conditions in P2-1 to reduce to

$(\forall p_1, p_2) \in P$, $p_1 p_2 \neq \emptyset$ and $\sim p_1 \sim p_2 \neq \emptyset$

(The other two conditions which imply $p_1 < p_2$ or $p_2 < p_1$ are satisfied trivially if $w(p_1) = w(p_2)$). But these conditions are equivalent to saying that p_1 or p_2 are each the complement of the other. Since the maximum number of points with weight $s/2$, satisfying this condition is

$1/2\binom{s}{s/2}$ we have shown:

<u>Theorem 1</u>: The solution to problem P2, for c=2, is given by $\underline{s}$ satisfying

$$\underline{s} = \min_s[1/2\binom{s}{s/2} \geq 2^n].$$

∎

Since $1/2\binom{s}{s/2} \simeq \dfrac{2^s}{(2\pi s)^{0.5}}$, $\underline{s} = O(n)$

Thus we get $K(n,2) = O(n)$ as was to be shown.

3. A Polynomial Bound on K(n,c)

In this section we will show that for each c, K(n,c) grows not more than with a polynomial of n, namely $K(n,c) \leq 2^c n^{c-1}$. This is a substantial improvement over the previously mentioned bound. To obtain this bound we will construct a set G of functions satisfying P1-1. The construction is a modification of one suggested to the author by R. Rivest who pointed out the existence of polynomial bounds for this problem.

Let U and V be sets of functions of n-1 variables. Let U x V be the set of functions of n variables defined as $U \times V = \{f \mid \exists u \in U, \exists v \in V, \forall(b_2, \ldots, b_n) \in \{\emptyset,1\}, f(\emptyset,b_2,\ldots,b_n) = u(b_2,\ldots,b_n), f(1,b_2,\ldots,b_n) = v(b_2,\ldots,b_n)\}$. Note that $|U \times V| = |U||V|$. Let $U = \{u_1,u_2,\ldots,u_p\}$ and $V = \{v_1,v_2,\ldots,v_p)$ be sets of functions of n-1 variables with $p = |U| = |V|$. Let U + V be the set of p functions of n variables defined as

$$U + V = \{f_i \mid \forall(b_2,b_3,\ldots,b_n) \in \{\emptyset,1\}, f_i(\emptyset,b_2,\ldots,b_n) = u_i(b_2,\ldots,b_n), f_i(1,b_2,\ldots,b_n) = v_i(b_2,\ldots,b_n)\}.$$

Let G(n,c) be a set of functions satisfying P1-1 for some n and c. G(n,c) can be constructed as follows:

1) Find all G(n-1,d), for d = 1,...,c.

2) $G(n,c) = \{G(n-1,c) + G(n-1,c)\} \cup \bigcup_{k=1}^{c-1} G(n-1,k) \times G(n-1,c-k)$.

The following is an immediate consequence of this definition.

<u>Lemma 3</u>: The set G(n,c) constructed as above satisfies P1-1.

From the above construction we get the following recurrence for K(n,c):

$$K(n,c) \leq K(n-1,c) + \sum_{1 \leq k \leq c-1} K(n-1,k) \,.\, K(n-1,c-k)$$

Using this recurrence we now show

<u>Theorem 2</u>: $K(n,c) \leq 2^c n^{c-1}$.

<u>Proof</u>: For c=1 we know K(n,1) = 2 so the theorem holds. Assume the result holds for all values of the second parameter less than c. Then, using the above recurrence,

$$K(n,c) \leq K(n-1,c) + \sum_{1 \leq k \leq c-1} 2^k(n-1)^{k-1} \,.\, 2^{c-k}(n-1)^{c-k-1}$$

Since the term inside the summation does not depend on k we get a new recurrence:

$$K(n,c) \leq K(n-1,c) + 2^c(c-1)(n-1)^{c-2} \quad \text{,so}$$

$$K(n,c) \leq 2^c(c-1) \sum_{j=1}^{n-1} j^{c-2} \leq 2^c(c-1)\,(n-1)^{c-1}/(c-1) \leq 2^c n^{c-1}$$

which proves the theorem. ∎

Since the number of control lines to select any of the $K(n,c)$ functions is $\log K(n,c)$ we get as a corollary:

Corollary 1: The number of exterior connections (besides those used for input) to a c-universal circuit is no more than $(c-1) \log n + c$.

Conclusions

In this note we have reexamined the problem of the number of exterior connections needed to control a circuit which is to be c-universal. For $c = 2$ we have found an exact solution and shown an upper bound for this number in the general case. The small bound found (of the order of $c \log n$ for the number of exterior connections) makes the implementation of these circuits very practicable.

References

[1] T. Lang and M. Schkolnick, "The Minimization of Control Variables in Adaptive Systems," in Theory of Machines and Computations, Z. Kohavi and A. Paz (eds.), Academic Press, 1971.